Vade Secure
Predictive Email Defense

FAQ ABOUT VADE SECURE FOR MICROSOFT 365

1. **What are the risks associated with email?**
   - 91% of cyberattacks start with an email.
   - Microsoft has been the #1 impersonated brand in phishing attacks for 5 straight quarters, thanks to the rapid adoption of Microsoft 365 (180 million users and counting). Microsoft 365 credentials provide a single entry point not just to the entire platform (e.g. OneDrive, SharePoint, Skype, etc.) but the entire business. Using compromised accounts, cybercriminals can launch insider attacks targeting anyone in the organization.
   - Successful email attacks inflict significant financial and reputational damage on small businesses and can disrupt or completely halt business operations. In fact, the FBI reports that more than $26 billion has been lost to business email compromise attacks over last 3 years.
   - A small organization can die in one successful attack. This is simply a factor of being unable to access financial, HR, production, sales, or customer data for several days.

2. **We have issues with phishing.**
   Can Vade Secure for Microsoft 365 help, or is it just another anti-virus and anti-spam solution?
   Vade Secure protects against all email threats: phishing, spear phishing, malware, ransomware, spam, scam, and low-priority mail (newsletters, purchase notifications, social media notifications, and travel-related content). Phishing is one of the most used malicious threats in today's cybersecurity world. To protect against phishing attacks, Vade performs two checks: one upon delivery of the email and another when the link is clicked – Time of Click (ToC). This protects against URL redirects in which the hacker redirects the user from a legitimate website to a phishing page. Vade detects redirects by performing a real-time page exploration and then posting a notification (customizable) to the user that the email has been classified as phishing.

3. **We have issues with spear phishing.**
   Can Vade Secure for Microsoft 365 help, or is it just another anti-virus and anti-spam solution?
   Vade Secure protects against all email threats: phishing, spear phishing, malware, ransomware, spam, scam, and low-priority mail (newsletters, purchase notifications, social media notifications, and travel-related content). Spear phishing, otherwise known as business email compromise (BEC), whaling, spoofing or CXO fraud, is a very dangerous attempt directed at a single person in the organization, typically to get money or information from an unsuspecting user. Vade Secure uses techniques like entity model queries, unsupervised anomaly detection, and natural language processing to defend against spear phishing threats. When a threat is detected, Vade Secure inserts a banner (customizable) into the email alerting the user to the spoofing attempt and suggesting that they contact the person by means other than email.

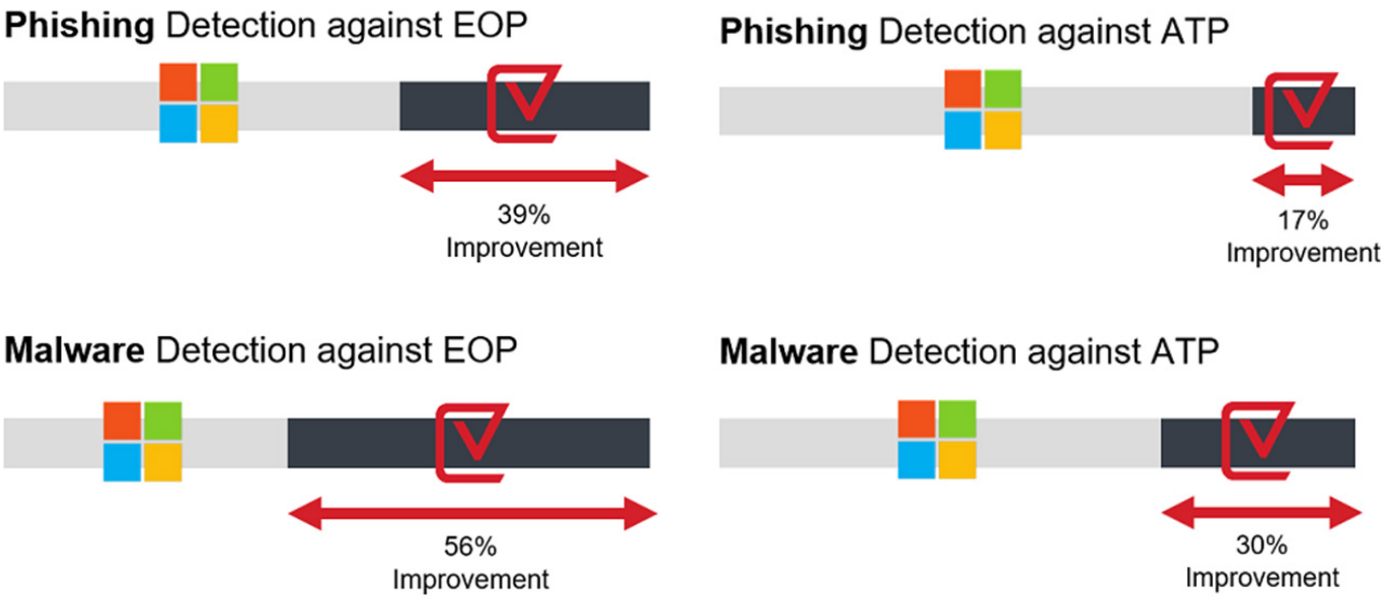
4. **Why should I add Vade Secure for Microsoft 365 to Microsoft EOP, which is free, or to ATP (Microsoft's premium add-on)?**

   Microsoft 365 is the market leader for cloud email platforms, which means that cybercriminals will constantly be reverse engineering Microsoft's built-in security (EOP) to break through these defenses. This is the premise for Gartner's prediction that by 2020, 50% of Microsoft 365 customers will rely on third-party email security solutions.

   Vade Secure for Microsoft 365 remains invisible to hackers because of its native, API-based integration with Microsoft 365. When hackers don't know which security solution you're using, they can't tailor their attacks to break through.

   Moreover, Vade Secure is a pure player in email security, spending 100% of its resources developing best-in-class, AI-based predictive email defense solutions. Vade's unique global footprint of 600 million protected mailboxes provides unparalleled access to threat intelligence, which enables them to train and refine highly accurate AI and machine learning models.

   In benchmarks against EOP and ATP, Vade outperformed both in terms of phishing and malware detection:



5. **We use and/or sell Microsoft EOP and/or ATP.**
   Does Vade Secure for Microsoft 365 work with these solutions?

   Yes. Vade is natively integrated with Microsoft 365 provides an added layer of security to EOP and ATP. Vade Secure provides a comparison report so you can see what is filtered and missed by Microsoft and what is filtered and caught by Vade. This is a valuable sales tool. Note that many traditional email security providers recommend disabling EOP and/or ATP because it creates email flow issues that affect the solution's effectiveness and impacts the end user.

6. **What are key differentiators of Vade Secure for Microsoft 365?**

   Competitors like Proofpoint, Mimecast, Forcepoint, Symantec, and Cisco are all cloud-based email gateways which sit outside the Microsoft 365 environment and require an MX record change. Vade Secure for Microsoft 365 is natively with Microsoft 365 via the Microsoft API. This approach offers several benefits over gateways:

   - **Instant provisioning:** The solution can be provisioned in minutes—no MX record change.
   - **Invisible to hackers:** MX-based products can be identified with a simple MX lookup, giving hackers an advantage. Vade remains invisible to hackers because it sits inside Microsoft 365.
   - **Uninterrupted user experience:** Vade filters messages into Outlook folders, based on defined policies, and there's no external quarantine—no end user training required!
   - **Insider threat protection:** Vade scans internal email traffic to protect against insider attacks that leverage compromised Microsoft 365 accounts.
   - **Layers with EOP:** Vade layers on top of Microsoft EOP. MX-based email security products require you to disable this built-in protection.
   - **Auto-Remediation:** Leveraging Vade's real-time view of emerging global threats, Auto-Remediate automatically removes any malicious messages from users' inboxes.

7. **What are other features does Vade Secure for Microsoft 365 offer?**

   - **Time-of-Click Anti-Phishing** – Crawls the URL and page in real time, following any redirections and analyzing the content and context of the URL/page to identify phishing. Admins can receive alerts when users click on phishing links, along with helpful training content to offer to the user.
   - **Banner-Based Anti-Spear Phishing** – Unsupervised anomaly detection and natural language processing scan for patterns, anomalies, and behaviors common in spear phishing emails. If an email is suspicious, a customizable banner is displayed in the message to alert the user.
   - **Behavioral-Based Anti-Malware** – Performs comprehensive analysis of the origin, content, and context of emails and attachments to identify polymorphic malware—without the long delays required by sandboxing technologies.
   - **Auto and One-Click Remediation:** Thanks to its real-time view of global threats, Vade can automatically remove any threats from users' inboxes. Admins can also remediate messages with one click.
   - **Comparative Report:** The comparative report quantifies Vade's added value over EOP and ATP and highlights threats it uniquely detected. The report is based on the client's live Microsoft 365 environment.
   - **Monitoring Mode:** In monitoring mode, Vade analyzes the email traffic but doesn't take any actions. This provides a no-risk way to test the solution and see what it catches in order to justify the purchase with clients.

8. **Why don't competitors offer an API-based solution like Vade Secure?**

   These big players offer a broader set of features beyond email filtering and threat detection, including encryption, archiving, and DLP. These technologies must be positioned at the MX record level. And, with archiving being the biggest driver of their revenue, making a change does not suit them.

9. **Can I test Vade Secure for Microsoft 365 without disrupting end users?**

   Yes. There are no changes to the user interface of Outlook, and the email flow does not change for end users. Additionally, Vade has two operating modes: monitoring and protection mode. In monitoring mode, analysis is performed and no action taken. This enables the administrator to review the solution without an impact to the organization. In protection mode, Vade performs that analysis and takes action on threats as determined by the policies configure by the system administrator.

10. **Does Vade Secure for Microsoft 365 ever have false positives?**
    False positives may happen in the event an alias is used for email notifications. Common false positive examples are 1) someone using their personal email, 2) a system automatically created an alias (i.e., Salesforce), and 3) a system automatically created tickets (i.e., IT, HR, marketing, development tools). Another example is an email security training company deliberately sending phishing emails to train a company's users. These scenarios can be avoided with white lists, by sender or domain, configured in two easy clicks.

11. **What tools does Vade Secure offer to facilitate customer management?**

- **Partner Portal** – Partners can manage clients and instantly provision free trials and production licenses for Vade Secure for Microsoft 365. They can also access marketing collateral and technical documentation.
- **Training Academy** – The Academy provides online, role-based training and certification for partner sales reps and sales engineers.
- **NFR License** – NFR licenses are offered free for one year and allow partners to protect their own employees' mailboxes, while gaining experience and confidence with Vade Secure for Microsoft 365.
- **Technical Support** – Partners have access to 24/7 email and phone support to assist with any inquiries or support issues.
- **Marketing Support** – Vade's marketing team works with partners to support demand generation activities, including the creation of co-branded assets and joint marketing programs.